

### **REMARKS**

Claims 1, 12 and 20 have been amended. Claims 4, 6, 10, 11, and 18 were previously canceled. Accordingly, claims 1 - 3, 5, 7 - 9, 12 - 17, and 19 - 29 are currently pending in the application and are presented for reconsideration and reexamination in view of the following remarks.

In the Final Office Action, claims 1 - 3, 5, 7 - 9, 12 - 17, and 19 - 29 were rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,747,564 to Mimura et al. in view of U.S. Patent Application Publication No. 2001/0001156 to Leppek.

By this Amendment, the Examiner's rejections have been traversed. Support for the amendments to claims 1, 12, and 20 can be found for example, in the specification at page 10, lines 5 - 7, and page 16, line 17 to page 17, line 8, for example.

It is therefore respectfully submitted that the above amendments introduce no new matter within the meaning of 35 U.S.C. § 132.

### **Rejection under 35 U.S.C. § 103(a)**

The Examiner rejected claims 1 - 3, 5, 7 - 9, 12 - 17, and 19 - 29 as being unpatentable over Mimura et al. in view of Leppek.

### **Response**

Reconsideration and withdrawal of the rejection are respectfully requested.

To establish a *prima facie* case of obviousness, the Examiner must establish: (1) that some suggestion or motivation to modify the references exists; (2) a reasonable expectation of success; and (3) that the prior art references teach or suggest all the claim limitations. Amgen, Inc. v. Chugai Pharm. Co., 18 USPQ2d 1016, 1023 (Fed. Cir. 1991); In re Fine, 5 USPQ2d 1596, 1598 (Fed. Cir. 1988); In re Wilson, 165 USPQ 494, 496 (C.C.P.A. 1970).

It is respectfully submitted that the combination of references fails to teach or suggest all the claim limitations.

The present invention discloses an asset protection system and method that integrates physical asset security with information asset security in a hosted environment, or in certain circumstances in a user's environment.

In the Advisory Action, the Examiner pointed out that argument concerning historic usage was not persuasive because the described feature is not claimed. While we believe that this feature is in fact described in the independent claims (usage pattern), we have amended the independent claims to provide additional language describing this feature.

Independent claim 1, as amended, recites, *inter alia*:

“...making access decisions in accordance with usage patterns of the user by using the integration of the processor based physical asset protection and processor based information asset protection to grant rights to the information systems...wherein the information asset protection reflects the user status change updated to reflect changes in security access requirements, and wherein usage patterns are calculated by comparing a present usage with historic usage...” (*emphasis added*).

Independent claim 12, as amended, recites, *inter alia*:

“...the integrator providing integration of the physical protection and information from the information asset protection module for making access decisions in accordance with usage patterns of the user to grant rights to the information systems...wherein the information asset protection reflects the user status change updated to reflect changes in security access requirements, and wherein usage patterns are calculated by comparing a present usage with historic usage...” (*emphasis added*).

Independent claim 20, as amended, recites, *inter alia*:

“...using an integration...for making access decisions in accordance with usage patterns of the user to grant rights to the information systems... wherein protection of physical and information characteristics of said asset is integrated in said centrally-located hosted environment, wherein the information asset protection reflects the user status change updated to reflect changes in security access requirements, and wherein usage patterns are calculated by comparing a present usage with historic usage.” (*emphasis added*).

Mimura et al. discloses a security guarantee method and system. As discussed in previous responses, Mimura et al. does not disclose processor-based physical asset protection or information asset protection as recited in independent claims 1, 12, and 20 of the present invention.

Mimura et al. also does not make access decisions as recited in independent claims 1, 12, and 20 of the present invention.

Further, Mimura et al. does not transmit a breach of physical asset protection in the centrally-located hosted environment as recited in independent claims 1, 12, and 20 of the present invention.

The Examiner cites Leppek in an attempt to cure the deficiencies of Mimura et al. regarding “making access decisions in accordance with usage patterns of the user” as recited in independent claims 1, 12, and 20.

Leppek teaches an integrated network security access control system. Further, the usage patterns of the particular user in Leppek are not learned; instead events are generated and monitored to establish a security association with the present activity for a user of interest. Thus, the controlled intervention in Leppek includes the ability to affect or modify a security association (ability to gain access) to another resource object.

In the present invention, a repeat system user’s usage patterns are “learned” to deny access if the present usage is an anomalous usage that results in corrective action. Further, as recited in the independent claims, usage patterns are calculated by comparing a present usage with historic usage.

In contrast, in Leppek, there is no discussion of a repeat system user, in other words, a user that has usage patterns, such that the present usage can be compared with historic usage, and then re-calculating the usage pattern.

Further, Leppek fails to cure the deficiencies of Mimura et al. regarding integration of physical and information security.

Furthermore, there is a lack of motivation to combine the security system of Mimura et al. with the one in Leppek because the combined teachings of those references would not have suggested the features of claims 1, 12, and 20 to those of ordinary skill in the art. The Examiner's conclusion of obviousness is based on improper hindsight reasoning because there is no motivation to combine these prior art references since the nature of the problem to be solved Mimura et al. is different from Leppek. In Mimura et al, the object is to improve security of a security object in a security zone that only specific persons are permitted to enter and leave and

to improve at a relatively low cost security of a security object in a security zone extending to a plurality of zones. In Leppek, the object is a new and improved network resource security access control mechanism that includes protection control, access control, event management and a proactive security agent routines integrated within the communications control software resident in a data communications network control processor, for controlling the ability of a network user to have access to and communicate with one or more information resources of the network.

Accordingly, Applicants respectfully request that the rejection of claims 1, 12, and 20, as amended, under 35 U.S.C. § 103(a) be withdrawn.

Moreover, as dependent claims 2, 3, 5, 7 - 9, 13 -17, 19, and 21 - 29, depend from one of claims 1, 12, and 20, Applicants submits these claims are also allowable for at least similar reasons.

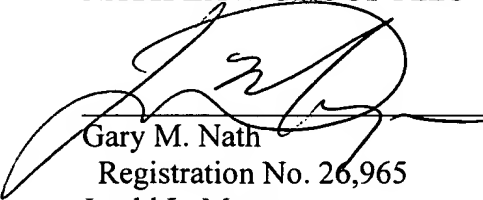
### CONCLUSION

In light of the foregoing, Applicants submit that the application is in condition for allowance. If the Examiner believes the application is not in condition for allowance, Applicants respectfully request that the Examiner call the undersigned.

January 25, 2007

THE NATH LAW GROUP  
112 South West Street  
Alexandria, VA 22314-2891  
Tel: 703-548-6284  
Fax: 703-683-8396

Respectfully submitted,  
**NATH LAW GROUP PLLC**



Gary M. Nath  
Registration No. 26,965  
Jerald L. Meyer  
Registration No. 41,194  
Teresa M. Arroyo  
Registration No. 50,015

Customer No. 20529